Chapter XXIV
Using Technology to Overcome the Password's Contradiction

Sérgio Tenreiro de Magalhães
Universidade Católica Portuguesa, Portugal

Kenneth Revett
University of Westminster, UK

Henrique M. D. Santos
Universidade do Minho, Portugal

Leonel Duarte dos Santos
Universidade do Minho, Portugal

André Oliveira
Universidade do Minho, Portugal

César Ariza
Bogomovil Ltda, Portugal

ABSTRACT

The traditional approach to security has been the use of passwords. They provide the system with a barrier to access what was quite safe in the analogical world. The digital era provided the means to easily try thousands of passwords in a short period of time and now the password schema is no longer safe. Now it suffers of the password's contradiction: the fact that it requires both simplicity and complexity to be usable and safe. Being so, new technologies are required that can preserve the easiness of use, but can provide stronger authentication processes. This chapter presents the latest advances in three technologies that can be used, unaided or together, to improve the safety of user/password schemas without significant changes in the protected information system architecture, despite the human factors that traditionally reduce the security of those systems. The presented technologies are Keystroke Dynamics, Graphical Authentication and Pointer Dynamic.

INTRODUCTION

Password vulnerabilities come from their misuse that, in turn, results from what we call the password's contradiction: the fact that a password must be both easy to remember, therefore simple, and secure, therefore complex. Consequently, it is virtually impossible to come up with a "good" password. On the other hand, once users have not yet completely realized the need for securing their authentication secrets, even fairly good passwords become a threat when the security policies (if at all existing) fail to be implemented. The results of an inquiry made in 2004 to sixty Information Technology (IT) professionals shown that, even among those that have technical knowledge, the need for passwords security is underestimated. This is probably one of the reasons why the governments increased their investment in biometric technologies after the terrorist attack of 9/11. But, although the use of biometric technologies to increase the security of a system has become a widely discussed subject, a consensus has not been reached. While governments and corporations are pressing for a wither integration of these technologies with common security systems (like passports or identity cards), human rights associations are concerned with the ethical and social implications of its use. This situation creates a challenge to find biometric algorithms that are less intrusive, easier to use and more accurate, while other solutions must be created/developed simultaneously.

In this chapter we present the latest advances in three technologies that can be used, unaided or together, to improve the safety of user/password schemas without significant changes in the protected information system architecture, despite all the human factors that traditionally reduce the security of those systems. The presented technologies are Keystroke Dynamics, Graphical Authentication and Pointer Dynamics.

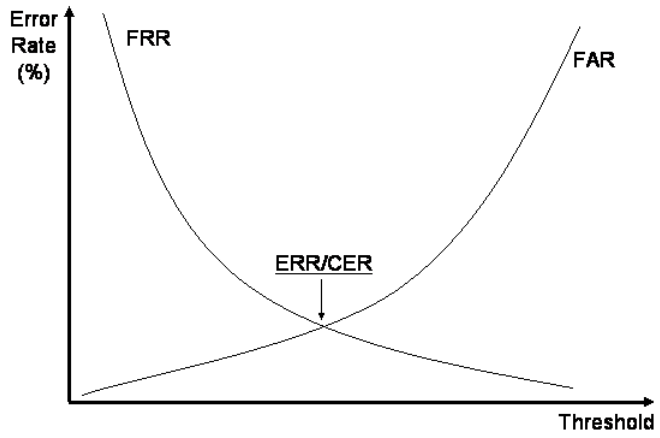
BACKGROUND: BIOMETRIC TECHNOLOGIES

Biometric technologies are mainly used in both physical and logical access control (Luis-García et al., 2003) but they can also be used to assist in other tasks, some so unimaginable has helping to preserve several animal endangered species (Jewell et al., 2001). But the use of biometric technologies to increase the security of a system has become a widely discussed subject and, while governments and corporations are pressing for a whither integration of these technologies with common security systems (like passports or identity cards), human rights associations are concerned with the ethical and social implications of its use (Privacy International *et al.*, 2004a; Privacy International *et al.*, 2004b). This situation creates a challenge to find biometric algorithms that are less intrusive, easier to use and more accurate.

The precision of a biometric technology is measured by its False Acceptance Rate (FAR), that measures the permeability of the algorithm to attacks, by its False Rejection Rate (FRR), that measures the resistance of the algorithm to accept a legitimate user, and by its Crossover Error Rate (CER), the point of interception of the FAR curve with the FRR curve that indicates the level of usability of the technology, also known as Equal Error Rate (EER). As an algorithm gets more demanding, its FAR gets lower and its FRR gets higher (Figure 1); usually the administrator of the system can define a threshold and decide what will be the average FAR and FRR of the applied algorithm, according to the need for security – dependent of the risk evaluation and of the value of what is protected; also the threshold can be, in theory, defined by an Intrusion Detection System (software designed to identify situations of attack to the system).

Establishing the error rates of a biometric technology is a complex problem. Studies have been made to normalize their evaluation, but the fact is that the results are strongly dependent of

Figure 1. False rejection rate vs false acceptance rate and consequent equal error rate, also know as crossover error rate



the number of individuals involved in the process and, what is worst, of who is chosen. This means that, even with a large amount of data collected, the results can be very different if we change the group evaluated. This happens because it's very difficult to obtain a sample representative of the population, once we do not know how to characterize the population. A good example of this disparity are the results of the Fingerprint Verification Competition (FVC) 2004, where the best CER achieved had a value of 2.07% (Maio et al., 2004), compared with the results of the FVC 2002, where the best CER achieved was 0.19% (Maltoni et al., 2003). Some international companies presented their products in both contests and the only justification for the disparity of the results is the difference in the sample data used to test the algorithms. All things considered, the only way to evaluate biometric algorithms is comparing them using the same data and, then, we can say that this technology is more accurate then that. The results also vary according to the use: a system used to identify an individual is less accurate that a system used to authenticate it (in this case the user presents himself to the system and it has only to confirm his identity)

Biometric technologies are usually classified as behavioral (e.g. voice recognition) or physical (e.g. retinal recognition), according to the classification of the characteristics evaluated. But they can also be classified as collaborative, if they demand that the user knows of its existence and participate in the process, or as stealth technologies, if they can be used without the knowledge of the one that is being authenticated or identified (Figure 2) (Tenreiro de Magalhães & Santos, 2005).

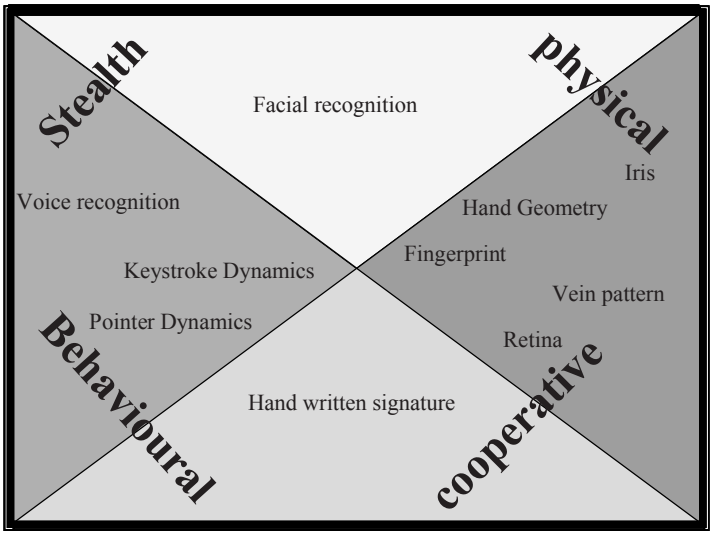
OVERCOMING THE CONTRADICTION ON PERSONAL COMPUTERS

Keystroke Dynamics

It is a biometrical authentication algorithm that tries do define a user's typing pattern and then verifies in each login attempt if the pattern exiting in the way the password was typed matches the user's known pattern.

The Keystroke dynamics algorithms are behavioral biometric technologies that can be used with the collaboration off the user or in stealth mode and that allows to increase the level of security, both in authentication and in identification, almost without any extra effort once it works by analyzing the patterns existing on the way that the user

Figure 2. Classification of biometric technologies: behavioural vs physical and stealth vs collaborative



types (a password, a passphrase or general text) on a keyboard. Furthermore, these algorithms can adjust their parameters to adapt themselves to evolutions on the typing patterns of the user

The approaches to find an algorithm that maximizes the performance of these technologies include, apart from the mathematical algorithms themselves, several different approaches to the information to be captured. The first keystroke dynamics algorithm dates of 1980 when Gaines presented a report of his work to study the typing patterns of seven professional typists (Gaines, 1980). The small number of volunteers and the fact that the algorithm was deducted from their data and not tested in other people later, results on a lower confidence on the FAR and FRR values presented. But the method used to establish a pattern was a breakthrough: a study of the time spent to type the same two letters (digraph), whenever together in the text. Since then, many others have used probabilistic calculations to improve the liability of the authentication process, especially in small texts like a passphrase or even a password and Gupta that, in 1990, presented an algorithm to calculate a value that represents the distance between acquired keystroke latency times and the correspondent times previously stored (Gupta, 1990). The development of the machine learning approaches allowed several sets of rules/classifiers to be found using, for instance, the similarity models of Bayes (Monrose & Rubin, 1997), the Rough Sets Theory (Revett et al., 2005) or neural networks (Revett et al., 2006a).

Keystroke Dynamics Accuracy

At this time several works have reached algorithms for keystroke dynamics that can achieve an Equal Error Rate/ Crossover Error Rate below 5%, which wouldn't be enough to guarantee the security of a system if it wasn't for the fact that this error rate is obtained after the password is made public, when in normal conditions (meaning without keystroke dynamics) it is a secret and if made public there isn't any other layer of protection. Tables 1 and 2 and Figure 3 show the precision of algorithms reached through the use of Rough Sets theory (Revett et al., 2006b), probabilistic neural networks (Revett et al., 2006a)and probability calculations based on the presumption of a distribution near to the Gauss Distribution (Tenreiro de Magalhães et al., 2005), respectively.

Table 1. A listing of the classification accuracy measurements (support and accuracy) for the rules obtained by (Revett et al., 2006b). The numeric values in the 'Support' column heading indicate the number of instances for each decision rule.

Support		Accuracy	
LHS	RHS	Decision: 1	0
55	55	100%	0%
59	59	100%	0%
49	48,1	97.9%	2.1%
39	38,1	97.4%	2.6%
41	40,1	97.6%	2.4%
43	42,1	97.7%	2.3%

Table 2. FAR/FRR values as a function of the division level, obtained by (Revett et al., 2006a). Note the values must be multiplied by 100 to give percentages.

Division points	False acceptance	False rejection
10	0.0483	0.0481
20	0.0192	0.0197
30	0.0576	0.0376
40	0.0576	0.0566
50	0.0576	0.0483
60	0.0001	0.0021
70	0.0576	0.0598
80	0.0481	0.0483
90	0.0288	0.0312
100	0.0480	0.0427

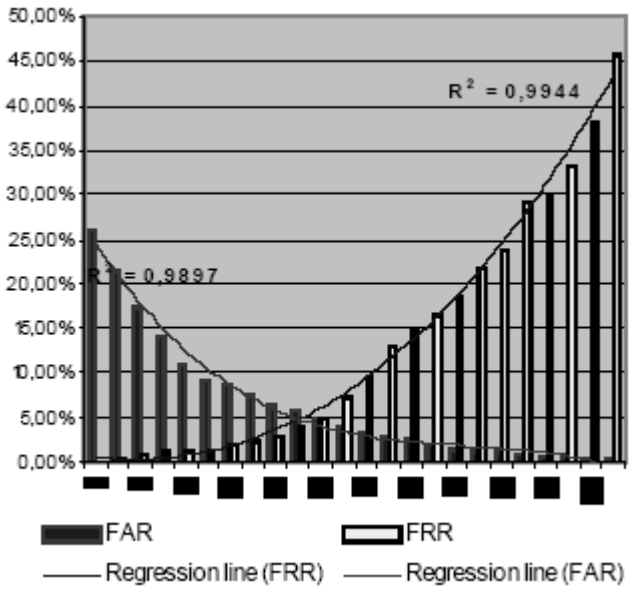
Future work should focus on retrieving what is best on the many approaches followed so far, in order to maximize the global effect.

Despite the improvement on security provided by keystroke dynamics, the situation is not altered when typing passwords using pointing devices like the palmtop stylus. In those situations we need to overcome the password's contradiction with a different approach.

OVERCOMING THE CONTRADICTION ON MOBILE DEVICES

In mobiles environments the level of privacy is normally higher, once the equipment is used nearer to the body of the user and/or the screen is smaller. Therefore, all the conditions are gathered to substitute passwords by graphical processes of authentication, taking advantage of the human ability to recognize visual information better

Figure 3. False acceptance rate and false rejection rate for several possible thresholds and estimation of the crossover error rate obtained by (Tenreiro de Magalhães et al., 2005)



than meaningless text-based strings (Nickerson, 1965; Shepard, 1967; Standing, 1973). Graphical Authentication is a technology in which the user selects some images from a bigger set, or selects some points in an image. The secret possessed by the legitimate user is the images/points selected and the corresponding sequence. These technologies can provide a way to generate traditional passwords, using unidirectional functions, from the sequence of images/points selected and, in this way, provide compatibility with the existing systems. Despite the fact that Blonder has patented the "graphical password" in 1996 (Blonder, 1996) many graphical systems have been proposed since then and in this section we will present some of the existing alternatives for using graphics instead of passwords, as well as our latest results on a pointer dynamics system, a biometric technology that goes beyond the secret inherent to graphical authentication by including behavioral biometrics in the authentication protocol.

Before stepping into section 4 we will also describe how Graphical Authentication Systems (GAS), while being used for authentication, can also be used to prevent phishing, a method for obtaining personal information (like passwords, Personal Identification Numbers, or others) in which a mail is sent to a user persuading him to follow a link to a page that is an imitation of a legitimate website. Once in there, the user is driven to provide the desired information. We will show that GAS can be used both to enhance the user's authentication procedures as to allow the user to authenticate the website.

Graphical Authentication Protocols

DAS - Draw a Secret (Jermyn et al., 1999)

This authentication scheme was drawn to be used in personal digital assistants - PDAs. In this scheme the personal code is a simple image drawn by the user on a grid. The drawing is converted in a sequence of pairs of co-ordinates. The text generated from the drawing is transformed using a unidirectional hash function and the result is

stored and associated to the user. The hash function from the registration process will be compared with the one stored in the system whenever the user tries to get access to the system.

The advantage of this method is that it originates long codes and the fact of being difficult to be imitated by other persons. Despite this scheme has been drawn with the objective of being using in PDA, it is also possible to use it in computers and, in this case, the use in public places is one of the disadvantages once that is easier to visualize and memorize a drawing in the monitor of a computer than to see what is being typed.

Déjà Vu (Dhamija & Perrig, 2000)

The authentication proposal elaborated by Dhamija and Perrig, is based on the generation of images having on is base a group of pre-selected images. This authentication scheme is composed of three phases: creation of the portfolio, training and, the last one, the login phase. The first consists in a selection of a group of abstract images. Starting with the selected images a process of generating new images is executed and those will be the ones to compose the user's portfolio. In the training phase, the user makes a small training with the objective to improve the image memorization. The last phase happens whenever the user tries to make the login. In this point the system shows a group of random images where the images of the user's portfolio are included and he must identify them.

The advantage of this process is that is practically impossible to describe the selected images and, once again, the disadvantage lies in the logins in public places.

Passfacestm (Real User Corporation, 2001)

This authentication scheme works in compliance with the empiric study of Brostoff and Sasse (Brostoff & Sasse, 2000)]. To create an access code it is required that the user pre-selects a group of four people's images among a group of images. After this, the users make a training process with the objective of memorizing them. In the login process a 3x3 grid is shown (nine images of people) in a set of four stages. Each stage contains an image from those pre selected and eight random ones. As can be seen, this authentication scheme is very identical to the previous outline (Déjà Vu), being that the previous scheme uses abstract images while PassFaces uses people's images.

The use of people's images is one of the disadvantages of this scheme once it is relatively easy to describe a person.

PassPoints (Wiedenbeck et al., 2005)

PassPoints is based on only one image for authentication in the system, in which the user should select a group of pre-selected and sequential points. In the authentication scheme, the user picks the pre-selected points, inside of a tolerance area defined around the selected point. The tolerance area is necessary once the choose point is a pixel, what is too precise for a human user.

Visual Identification Protocol (VIP)

(De Angeli et al., 2003)

Angeli proposed a solution for user authentication based in images and in the user's visual memory (De Angeli et al., 2003). Three authentication processes were created in this solution and compared with the PIN, Personal Identification Number, process (table 3). The first possibility (VIP1), consisted in the selection of four images from a group of 10 pre-defined images, disposed in fixed positions and introduced in the same order, or disposed in random positions (VIP2). In the last process (VIP3) the limits of the visual paradigm are studied. The user has a portfolio of 8 images, and in each authentication attempt four images among the eight images are shown together with 12 random images (of distraction images) and the user has to identify his images without any specific order. Angeli's study showed

that the most common mistakes associated with VIP1 were related with a wrong sequence selection, in VIP2 the mistakes were due to a wrong sequence of images and wrong identification of the images, and in VIP3 most of the mistakes were due to a wrong identification of images, that is, the user tended to identify distraction images as being part of his portfolio.

Magalhães, Revett E. Santos (Magalhães et al., 2006)

This system, proposed in 2006, consisted in the choice of an image of among four made available. Each image includes a grid (20 x 15) in which each area can be seen as a pair of letter/number, where the first line contains letters and the first column contains numbers. The user must choose between the graphical secret key and the traditional secret key based on text. Having chosen the image, the user must select the several areas that compose his personal code. After the selection of the several areas, the system transforms the several points in an alphanumeric text. This scheme diverges from the PassPoints scheme, in the fact that the user selects a set of fixed and known areas while in the latest the user selects a group of points (pixels) of an image.

Best Practices in Choosing the Images

The use of a graphical authentication system eliminates some problems related to the alphanumeric codes, however, also potency possible bad habits related with this new authentication form. Magalhães et al elaborated a study (Magalhães et al., 2006) in which they tried to understand the user's methods of choosing images and areas inside an image.

The results obtained with the experience were surprising, having attained a group of important factors which should be considered when maximizing the safety of the graphical authentication process. The results showed that:

- 50% of the user defined codes had less than four points and, from those, 70% didn't have more than five points. Of notice: 21% of the codes had only one point in only one image.
- 75.9% of the codes had only points in the same line (55.5%) or in the same column (20.4%).
- of the totality of the chosen points, the next line to the one of the letters, the corners of the images, the people's eyes, the letters and the numbers obtained respectively, 39.94%, 13.12%, 9.18%, 10.06% and 6.56% of probability of being chosen to belong to a code, instead of 6.67%, 2.11%, 0.83%, 6.67% and 5.26%, respectively, expected if random.

The conclusions from this study showed that the analysts and the programmers need to implement the correct security policies, forcing users to follow and respect a group of rules of graphic codes definition, for instance:

- To force users to introduce codes with at least 5 points.

Table 3. Authentication processes and results

Prototype	Type of code	Location	Security scoring
VIP1	4 fixed order images from 10	Fixed	Same as PIN
VIP2	4 fixed order images from 10	Random	Intermediate
VP3	Portfolio based	Random	Maximum

- To prohibit the definition of codes with points in the same line and column or corners
- Not to propose images with people and with points standing out from the global image (when the images are not uploaded by the user but, has it has been common, are proposed by the system).

Generating a Password from a Passgraph

A passgraph with length n will be a vector of the type $(p_1, p_2,..., p_n)$ where $p \in \{(x,y) \mid 0 \le x \le 19,\ 0 \le y \le 13\}$. The values of x and y define the selected section in a specific two-dimensional image. In order to maintain the compatibility with the traditional password systems, we need to generate a string. For that, we'll use 15 tables, numbered from 0 to 14, with 26 columns and 20 lines. So we have 7800 cells, each one with one 3 characters string and the corresponding ANSI code. Table 4 is one of those tables.

We find our first cell by locating, in the number (x+y)mod15 table, the line x and column y. Then, for each $p \in \{(x,y) \mid 0 \le x \le 19,\ 0 \le y \le 13\}$ we'll do:

$$\left(x + y + 1^{st}\ ANSIFromThePreviousSelectedCell\right) mod\ \ NumberOfLines$$

to find the next line selected;

$$\left(x + \bar{y} + 2^{nd}\ ANSIFromThePreviousSelectedCell\right) mod\ \ NumberOfColums$$

to find the next column selected;

$$\left(x + \bar{y} + 3^{rd}\ ANSIFromThePreviousSelectedCell\right) mod\ \ NumberOfTables$$

to find the next table selected;

To prevent the possibility of discovering the sequence of clicks from the string if this is compromised, for instance by capturing the packages on a poorly encrypted network, we need to make some final changes in the string. In this way, frequent changes in the tables (and the correspondent passwords) can increase the level of security of the system, in a transparent way to the user that will continue to click in the same places of the same figures. In our case:

Let x be the ANSI code of the first element of the so far generated string. Given t = x mod n, will reverse the order of the first t characters.

Let y be the ANSI code of the last element of the so far generated string. Given k = x mod n, will reverse the order of the last k characters.

If the system allows the user to choose at the moment of login what system to use according to the surrounding environment and/or used device, then there must be a way to convert the passgraph to the user's password. This can be achieved in two ways: the system accepts two different passwords, the one chosen by the user and the one that

Table 4. The conversion of the passgraph to traditional passwords (creating strong passwords) is made through unidirectional functions that make use of 15 tables similar to this one

0																									
4kQ	v9:	D'l	~\'	M'p	K"l	.n.	@8v	(!p	LQi	H=p	i.6	h$m	.:]	g:	]h8	D-(	-Yh	`Ri	T^-	evf	v6:	i*f	iJH	^sI	{(T
E6W	xnf	:)V	Sx8	e(r	XT0	:8u	aW A	x6w	pd/	#.T	t4j	EwB	.:^	EIX	VQU	PiE	br4	wch	.!I	A:/	*eb	D.S	8R1	8%i	dQi
B`o	)5N	yDv	y$U	.:3t	F`]	[+-	X!g	yvd	HdF	9XQ	Wcp	2-u	pEB	}Tj	jZ!	mx	f#I	5Df	&)^	?d$	up6	3:@	u=	r<	vjK
T~3	LZM	hF7	'V	]`d	C)(	-5%	]:3	qwn	&!n	-vf	sTr	IrV	X3d	aZn	zs4	HqV	i1U	@v>	AUs	L[a	?/n	OkA	lS/	=s/	j<6
ZU8	xtx	vT2	ekN	Evy	V^#	)I2	2Fv	<w&	u(=	l6L	?f0	\r.	Jew	6l/	zL]	`Oc	zJk	Ati	Y&h	xG\	O]^	L3E	P#D	8.d	tfx
!Z[	He$	'Ot	HdS	QB(	>.v	ewC	]\(d	avq	%+"	a")	0LY	DE	NiD	53l	xXV	rv6	~ Y	:l6	((e	$.8	D~2	Mp	IL9	-zI	Ad~
aC&	@.H	ios	Hq4	e$Q	(i?	0fl	k;n	hpS	Dx$	z0&	?P3	W#f	k;B	&k`	v#^	O/t	0)g	48a	4~I	sv\	N.!	qZb	~"J	?/<	zaL
~t	0lp	:%S	%$K	bUb	`f-	`9(	3"'	u<W	HKl	@m=	CTQ	O)H	no:	A-t	{l#	Q\)	rGc	1TX	lVy	`<o	l7B	~Np	"."	3^$	gYr
P?p	x7U	&^"	FLn	Fl.	.\b	1jo	4(E	l.$4	##	6Bv	h8]	e@J	KFP	cO&	)SN	$kS	fN!	b(!	-%w	jl/	c7`	#P·	:an	2=!	q^4
k2"	v0n	z$S	v4i	W.?.	.yL	$#u	-g)	&O}	wZt	\G[	l5B	k\a	BK6	Xhp	m=c	[(Q	Tkd	+!r	!Y^	IMf	KVf	iiM	riJ	tF#	+v(
-md	eYY	t4Y	ali	y]!	cT6	MI@	wsk	8Bo	iES	l9R	#&	N.k	:??	(*V	h*i	0@^	^1"	xB$	-lv	<.t	Kb/	V9<	&2m	:.0	D#r
ZVW	i.W	X~O	//3	g@5	o%h	rAM	kuv	BI9	xzb	UQR	4"b	gIN	S6*	@6\	il6	UMr	z"H	n.K	O-H	8el	<>r	4H2	f//	p;P	ZVw
WKA	.y>	?"B	XDw	+g.	OQ*	DNL	]d1	9If	A[7	/Y'	j8\	h]1	CF*	DV:	tot	(>~	]4H	v%3	V[o	*s	!5Q	ey&	$o\	d(%	o(@
]04	e5Y	$rB	&g@	~~E	?<!	3]/	ZG	"MD	9t[	{DF	jzU	D`d	6B~	Z?]	tjl	8g+	RFi	~W3	s7F	?Sj	]V{	`RS	.5g	xke	dqO
"M:	OCn	G%k	wyv	R~o	9kb	7uM	qCa	.|.	2G1	'Ew	CFi	Ljz	v+d	#1&	/e$	oxG	-o2	U`i	3k!	<2g	#wE	<ub	Z2T	lq$	zK'
qqz	t4%	\a:	J\2	([	kv>	lkl	K07	&6x	:N:	>5V	)eq	>L2	2su	Cb^	M)(	3?T	Z]*	-^D	qUr	>Ll	=C:	rMS	b^~	>6/	pte
W&H	!bQ	:W w	dbX	P6U	AkE	`7K	G#%	u6V	TN9	A;3	1Q(	.L5	Gm-	@HA	'ic	Zs[	>N/	c;?	n.>	0rW	5\)	qQ(	B3[	*Bh	#Ti
!~z	UxU	veV	H~?	:b#	S80	:=?	HXd	^H~	yI1	Tt*	.db	V)7	Ff!	XYt	P=W	iKO	t-3	w1l	ubN	W sk	\Ko	W 8x	ybu	+g2	]).
Ud.	@yL	ccl	tba	1wP	sXB	LGk	-'A	sSC	dxU	~6Z	A6r	7[m	1v%	R'M	"7]	~`k	W &5	lXl	62]	tDn	V#R	LLj	pHp	XHm	v=G
)C!	a;E	<qM	QG#	w(@	M&.	[<@	!QP	vn*	*D~	s2W	v4@	VJ'	do*	TU"	.<B	SRA	x9t	K.I	DzC	6-	S.8	~Q]	),?	N^)	hVY

will be generated from the passgraph; or there is a conversion table that allows the processing (on the server's side) of the data coming from the authentication fields and tests both the password at it is and the corresponding conversion result. This table would associate to each user a table containing the character associated to each of the trigraphs existing in the conversion tables (see Table 4). Each character of the alphabet is, of course, repeated several times and this table will not give any clue to the user's password. In this case the quality of the generated password is reduced to the exact level of security provided by the user's password, once they will be the same.

POINTER DYNAMICS

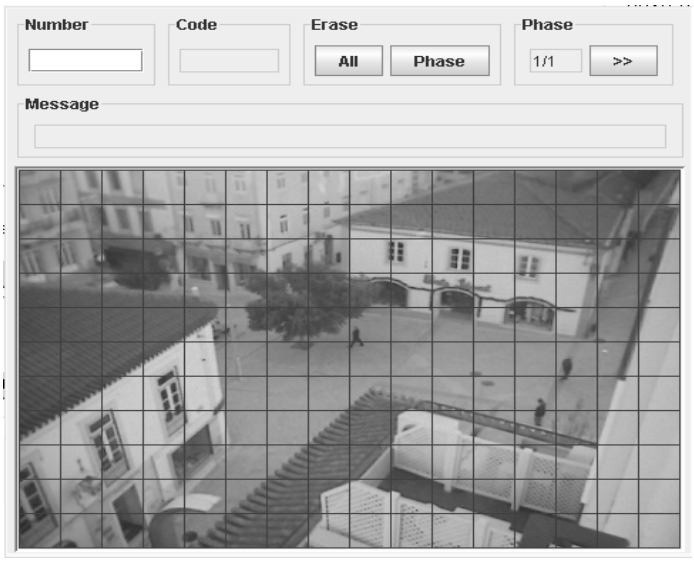
This is an experimental concept in which a biometric algorithm aims to define a user's clicking pattern when using a pointing device (mouse, stylus, touch pad, etc.) to authenticate towards a Graphical Authentication System. In each login attempt, access is granted if and only if the pattern exiting in the way the secret was clicked matches the user's known and recorded pattern.

An Experimental System

In order to test a Pointer Dynamics authentication process we integrated a java applet in a software called Moodle, a Course Management System. The login process, in the software Moodle, was transformed in order to integrate and substitute the conventional user and password by the one generated by our developed java applet. To support Moodle we have used a software package called WAMP5 that has among others MySQL as database, Apache as web server and PHP.

Both the enrolment and the authentication environment consist on a window with a field for a username, a dialog panel, where the users get feedback from the system; two buttons to erase the password and a third button used only in the enrolment process. The enrolment consists in 12 steps in which the user has to repeat in each one the graphical secret so that the system has a set of times required to establish a pattern. The image was divided in an 11x16 grid (Figure 4) and in the java applet was implemented a few limitations based on the study of Magalhães et al(Magalhães et al., 2006):

Figure 4. The registration and authentication system



- The passwords must have at least 4 points and at the most 10 (this one implemented for reasons related to the moodle's architecture).
- The passwords points couldn't be all in the same line or in same row.
- The passwords points couldn't be all in the corners.

Also, the image used for the experiment was selected in accordance with the rules proposed in the study of Magalhães et al(Magalhães et al., 2006). In order to make the process of describing the authentication graphic secret to a third person more complex, no identification was included in each column or row.

Obtained Accuracy

For the experiment we have used 9 users from different professional areas, which provided their user and graphical secret (passgraph) information after registering in the system. Then, a group of university students from different grades tried to access the system, using the known login data.

To understand if the times between clicks were information enough to provide the system with an authentication pattern, we used an algorithm developed for keystroke dynamics.

The used algorithm has two distinct phases: the enrolment and the authentication attempt. In the enrolment phase, the user clicks his secret key twelve times and the systems records the times spent between the several clicks, calculating the average, the median and the standard deviation for those twelve times. The authentication attempt phase consists on, for each two points clicked, collect the proposed (once the alleged user is proposing that time as a legitimate one) time spent – PTS – and compare it with the corresponding value stored during the enrolment stage through the acceptance criteria presented in Figure 5, where α is a definable parameter.

Once all the times corresponding to the sequence of clicks constituting the secret key were classified, they received the value of 0 (zero) if they didn't satisfy the criteria, 1 (one) if the time satisfies the criteria and the time before didn't (or if it is the first time evaluated) and 1.5 (one point five) if it satisfies the criteria and so did the time before. Those values were added together and the final sum A corresponded to the level of trust in the presented pattern. If the value A is not smaller then the defined threshold (a defined parameter) then we would accept the user as legitimate and replace the oldest stored time sequence by this one, therefore allowing some evolution in a user's pattern. The obtained accuracies, with α set at 0,6 (zero point six), for the different thresholds are presented in Figure 6, along with the corresponding tendency lines (polynomials of 6th degree).

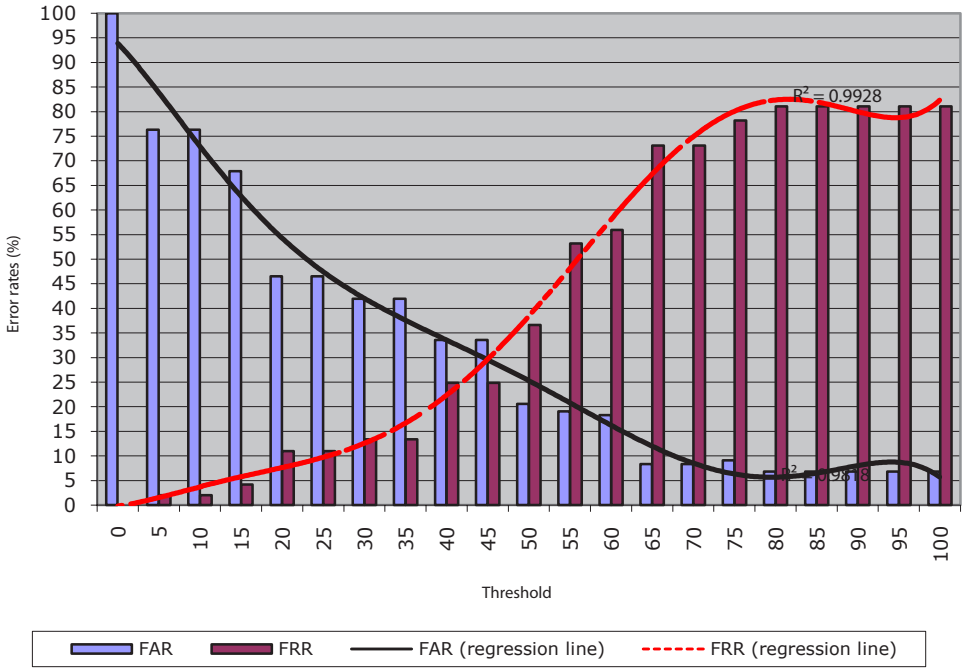
The Crossover Error Rate (CER) proved to be very high (approximately 30%) but the fact that low False Acceptance Rates and low False Rejection Rates were achievable (not at the same time) clearly indicates that this is a valid technology that, of course, need time and work to find new algorithms that will lead to an acceptable level of maturity.

Another fact observed was that, despite the initial efforts, several users chose a diagonal secret key. Therefore, it was decided to verify what would happen to the accuracy levels if only the users' with secret keys dependent on the image,

Figure 5. Acceptance decision criteria for a given time input

$$Lowest(Average; median) * \left(1 - \alpha - \frac{Sdeviation}{Average}\right) \leq PTS \leq Higher(Average, median) * \left(1 + \alpha + \frac{Sdeviation}{Average}\right)$$

Figure 6. Obtained accuracy for the test algorithm with α set at 0,6 (after the secret code was made public)



not on geometry, were considered. The results improved a lot and the CER dropped bellow 19% (Figure 7).

The results indicate that one must be very careful when implementing the security policies for the constitution of the secret access keys and that, if so, one can obtain very satisfying levels of accuracy.

Using GAS to Authenticate Both the User and the Service

When surfing on the Internet one must authenticate in order to access restricted areas, but there is no authentication for the website soliciting the user's authentication data. Several attacks can mislead the user into thinking that he is entering the authentication data on one determined website when in fact he is entering the data on someone else's site, designed to impersonate the original one. That can be achieved in many ways, for instance by DNS cache poisoning or DNS Hijacking (Wüest, 2005). One of the first entities to realize this need for an authentication of the website was the Bank of America that presented in 2005 the PassMark system, designed with the objective of allowing the user to authenticate the website by recognizing one determined mark that is particular to him and that was previously chosen (Bank of America, 2005). What we propose is that the images used to authenticate the websites can also be used as a basis for the user's authentication. In our proposed system, when a registered user intends to access the service, he inserts his username and the system creates the corresponding login page that includes the image that is specific to that user and, inserted on the image, the Internet Protocol address (IP) of the machine that requested the image (Figure 8) and the date/time of the request (to prevent reutilization of the image for fixed IP machines). If the system does not present the correct image, the correct date/time or the correct IP, the user knows that he is most probably dealing with an impersonation of the server acting as the

Figure 7. Accuracy level for the users that have a secret key (made public) dependent of the image

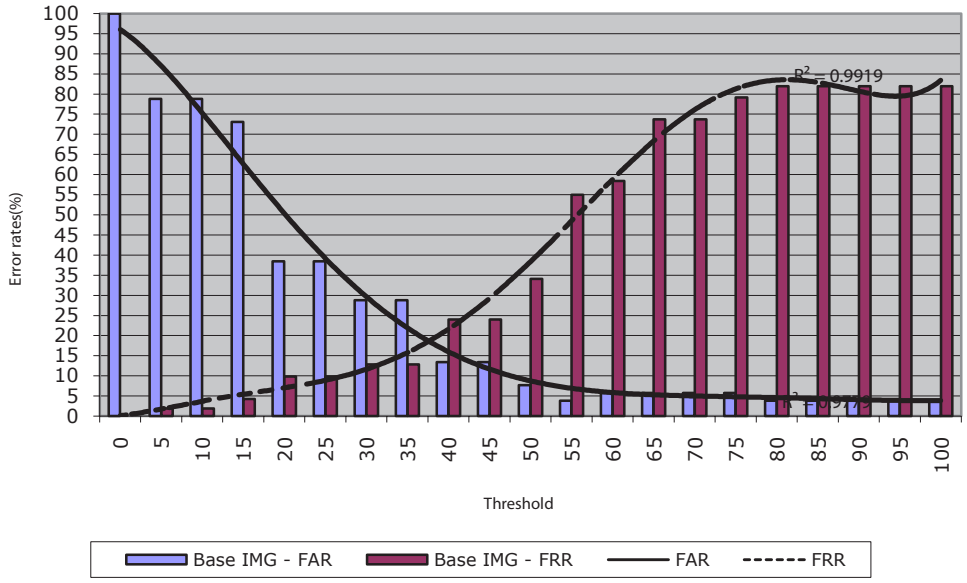
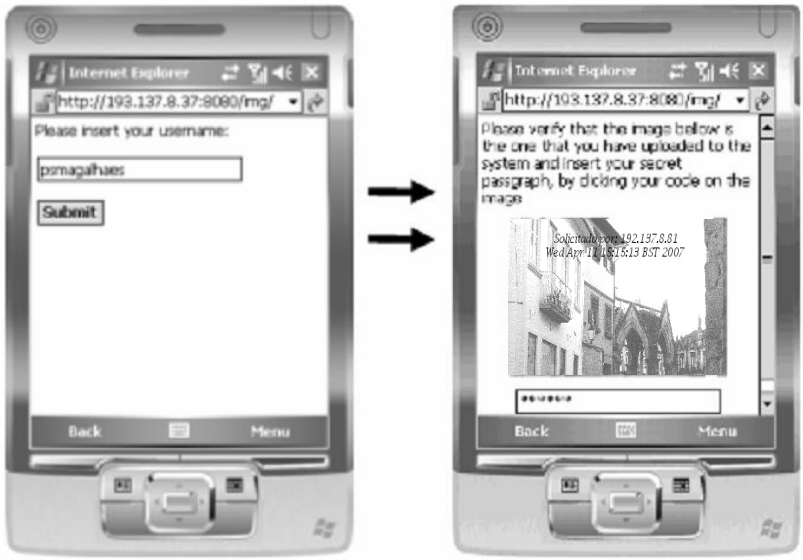


Figure 8. Pointer dynamics authentication system



"man in the middle" and does not proceed with providing the authentication data. In this way, the GAS is being used for the authentication of both the user and the site. This process protects the user from malicious software like PWSteal.Bancos.B (also known as Infostealer.Bancos.B) that creates an authentication windows over the original one in order to capture the authentication data outside the protection of the SSL protocol despite the presence of the SSL padlock with the correct certificate details (Symantec Corp., 2003), once the authentication image would be

covered. Unfortunately this cannot provide any additional protection against Trojans that, when detecting the access to a known website, store the sequence of clicks and a screenshot, allowing the calculation of all the positions clicked. The other drawback of this system is the possibility of having the IP changed along the communication, leading to information of the image that can be deceiving. This can be made, for instance, when using proxy servers.

FUTURE TRENDS

The research in the field of behavioural biometrics has grown is the past few years, mainly due to the potentiality of any large scale authentication process that does not require any dedicated hardware. This characteristic is even a requirement when the context is a service provided through the Internet for the withiest audience possible. Considering the usability of the presented technologies, future research will focus on three essential aspects: the accuracy of the authentication algorithm, the evolution from authentication to identification and the protection of the private data when using the technology in crowded spaces.

The accuracy of the algorithms will continue to improve along with the evolution of the mathematical theories that support that research. At the same time, new approaches for the use of the technology will improve the acceptability of the processes and help to solve other problems, like stepping from authentication, when the user presents himself as the legitimate owner of a system's, to identification, when the system detects, by itself, the correct identity of the user. Recent studies show that graphical authentication, when the selection of the images/sections is performed not through touching the screen but using the keyboard, can be less prone to shoulder-surfing then traditional passwords (Tari *et al.*, 2006). Other fields of research have presented works that are trying to solve the shoulder-surfing problem from different perspectives, for instance by allowing the selection of the images/sections to be made only by looking at them, thanks to an eye-tracking system (Hoanca & Mock, 2006). All these solutions will continue to increase the potential of the technologies destined to overcome the password's contradiction but will require an extra effort to improve the accuracy of the resulting algorithms, once all those evolutions will have a negative effect on it.

CONCLUSION

The several results and schemas presented along this chapter allow us to conclude that, if the human factors associated to the use of passwords are taken into account, it is possible to provide easy to use and non-intrusive technologies that can enhance the existing authentication schemas security, without demanding more effort from the users and, in some conditions, these schemas will also prevent other kinds of attacks like phishing.

At this moment, overcoming the password's contradiction requires the use of a behavioral/stealth biometric technology—Keystroke Dynamics—and graphical authentication (when using mobile devices), but in the future graphical authentication can become usable in open spaces, due to the integration with eye-tracking systems and/or by using them through the keyboard. Biometric technologies can also be applied to graphical authentication with some success, but not yet completely satisfying, and future research in the quest for better algorithms and in the understanding of the user's behavior can considerably improve their performance. At the same time that one overcomes the password's contradiction applying to graphical authentication, a serious advance in authenticating the provider of the service is also made, providing a higher level of trust to the systems.

REFERENCES

Bank of America. (2005). *Bank of America announces industry-leading security feature for its 13.2 million online banking customers to help prevent fraud and identity theft.* Retrieved April, 2007, from http://newsroom.bankofamerica.com/index.php?s=press_releases&item=6971

Blonder, G. E. (1996). Graphical password. In US (Ed.): Lucent Technologies Inc. Murray Hill, N. J.

Brostoff, S., & Sasse, M. A. (2000). Are passfaces more usable than passwords: A field trial investigation, *HCI 2000*: Springer.

De Angeli, A., Coventry, L., Johnson, G. I., & Coutts, M. (2003). Usability and user authentication: Pictorial passwords vs. Pin. In P.T.McCabe (Ed.), *Contemporary ergonomics 2003* (pp. 253-258). London: Taylor & Francis.

Dhamija, R., & Perrig, A. (2000). Déjà vu: A user study using images for authentication. *9th USENIX Security Symposium*.

Gaines, R. (1980). *Authentication by keystroke timing: Some preliminary results* (No. Report R-256-NSF): Rand Corporation.

Gupta, J. (1990). Identity authorization based on keystroke latencies. *Communications of the ACM, 33*(2), 168-176.

Hoanca, B., & Mock, K. (2006). Secure graphical password system for high traffic public areas. *Eye Tracking Research & Applications Symposium 2006*. San Diego: ACM SIGGRAPH.

Jermyn, I., Mayer, A., Monrose, F., Reiterand, M., & Rubin, A. (1999). The design and analysis of graphical passwords, *8th USENIX Security Symposium*.

Jewell, Z. C., S. K., A., & Law, P. R. (2001). Censusing and monitoring black rhino (diceros bicornis) using an objective spoor (footprint) identification technique. *J. Zool*(254), 1-16.

Luis-García, R., Alberola-López, C., Aghzout, O., & Ruiz-Alzola, J. (2003). Biometric identification systems. *Signal Processing, 83*, 2539-2557.

Magalhães, P. S., Revett, K., & Santos, H. D. d. (2006). *Critical aspects in* authentication graphic keys, *International Conference on Information Warfare and Security (ICIW2006)*. Maryland Eastern Shore, USA: Academic Conferences, Inc.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2004). Fvc2004: Third fingerprint verification competition, *International Conference on Biometric Authentication – ICBA*. Hong Kong.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2003). *Handbook of fingerprint recognition*. New York: Springer.

Monrose, F., & Rubin, A. D. (1997). Authentication via keystroke dynamics, *Fourth ACM Conference on Computer and Communication Security*. Zurich, Switzerland: ACM.

Nickerson, R. S. (1965). Short-term memory for complex meaningful visual configurations: A demonstration of capacity. *Canadian Journal of Psychology, 19*, 155-160.

Privacy International, Statewatch, & European Digital Rights. (2004a). *An open letter to the icao a second report on 'towards an international infrastructure for surveillance of movement'*. Retrieved January, 2005, from www.privacyinternational.org

Privacy International, Statewatch, & European Digital Rigts. (2004b). An open letter to the european parliament on biometric registration of all eu citizens and residents. Retrieved January, 2005, from www.privacyinternational.org

Real User Corporation. (2001). The science behind passfaces. Passfaces^{tm}. Retrieved October 2005, from http://www.idarts.com/

Revett, K., Gorunescu, F., Gorunescu, M., Ene, M., Tenreiro de Magalhães, S., & Santos, H. D. (2006a). Authenticating computer access based on keystroke dynamics using a probabilistic neural network, *2nd Annual International Conference on Global e-Security*. London: University of East London.

Revett, K., Magalhães, S. T. d., & Santos, H. (2006b). Datamining a keystroke dynamics based biometrics database using rough sets, *EPIA 2005, Portuguese Conference on Artificial Intelligence*. Covilhã, Portugal: IEEE CS Press.

Revett, K., Tenreiro de Magalhães, S., & Santos, H. D. (2005). Developing a keystroke dynamics based agent using rough sets, *International Workshop On Rough Sets And Soft Computing In Intelligent Agent And Web Technologies*. Compiègne: University of Technology of Compiègne.

Shepard, R. N. (1967). Recognition memory for words, sentences and pictures. *Journal of Verbal Learning and Verbal Behavior, 6*, 156-163.

Standing, L. (1973). Learning 10,000 pictures. *Quarterly Journal of Experimental Psychology, 25*, 207-222.

Symantec Corp. (2003). Infostealer.Bancos.B. Retrieved April, 2007, from http://www.symantec.com/security_response/writeup.jsp?docid=2003-073117-3108-99

Tari, F., Ozok, A. A., & Holden, S. H. (2006). A comparison between of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. *Symposium on Usable Privacy and Security (SOUPS) 2006*. Pittsburgh, PA, USA.

Tenreiro de Magalhães, S., Revett, K., & Santos, H. (2005). Password secured sites - stepping forward with keystroke dynamics, *International Conference on Next Generation Web Services Practices*. Seoul, Korea: IEEE CS Press.

Tenreiro de Magalhães, S., & Santos, H. (2005). An improved statistical keystroke dynamics algorithm, *Multi Conference on Cumputer Science and Information Systems*: IADIS.

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Basic results, *Human-Computer Interaction International (HCII 2005)*. Las Vegas.

Wüest, C. (2005). "Phishing in the middle of the stream" - Today's threats to online banking. *8th Annual AVAR International Conference*. Tianjin, China.

KEY TERMS

Authentication: It's the process of verifying the identity alleged by a user that tries to gain access to a system.

Collaborative Biometric Technology: It's an authentication biometric authentication technology that requires the user's volunteer and intended participation in the process. It opposes to the stealth biometric technologies that can be used without the user's consent.

Crossover Error Rate (CER): Authentication algorithms need to simultaneously minimize the permeability to intruders, therefore they have to be demanding, and to maximize the comfort level, therefore to be permissive. This contradiction is the base for the optimisation problem in authentication algorithms and the measure of success for the overall precision of an algorithm and of its usability is the Crossover Error Rate (CER), the error rate obtained at the threshold that provides the same False Acceptance Rate and False Rejection Rate.

False Acceptance Rate (FAR): This rate is a measure of the permeability of an authentication

algorithm. It's calculated by dividing the number of intruder's successful login attempts, by the total number of intruder's login attempts.

False Rejection Rate (FRR): This rate is a measure of the comfort level of an authentication algorithm. It's calculated by dividing the number of unsuccessful attempts made by the legitimate users, by the total number of legitimate login attempts.

Graphical Authentication System: It's a login system that verifies the user's knowledge on specific images or parts of images to grant or deny him a successful login.

Identification: It's the process of discovering the identity of the user that tries to gain access to a system. It's differs from authentication because in the identification process no identity is proposed to the system, while in authentication an identity is proposed and the system will only verify if that identity is plausible.

Keystroke Dynamics: It's a biometrical authentication algorithm that tries do define a user's typing pattern and then verifies in each login attempt if the pattern exiting in the way the password was typed matches the user's known pattern. Another application of Keystroke Dynamics, at least in theory, is the permanent monitoring of the user's typing pattern in order to permanently verify if the user that is typing is the legitimate owner of the system's account being used.

Passgraph: It's the user's secret code to access a system protected by a graphical authentication system. It is constituted by a sequence of points where the user must click in order to obtain a successful login.

Stealth Biometric Technology: It's an authentication biometric authentication technology that can be used without the user's consent. It opposes to the collaborative biometric technologies that require the user's volunteer and intended participation in the process.

Threshold: It's the variable that defines the level of tolerance of an algorithm. It can be set on a more demanding value, raising the False Rejection Rate and lowering the False Acceptance Rate, or it can be set on a less demanding error, lowering the False Rejection Rate and raising the False Acceptance Rate.